

REMARKS

Oath/Declaration

The Examiner states the Oath and Declaration is defective because it was not signed. Enclosed is a copy of the signed declaration submitted in Response to a Notice of Missing Parts on May 15, 2002. Additionally, Applicants also submits a copy of the transmittal and return receipt postcard that accompanied the submitted Declaration.

Specification

The disclosure is objected to because a serial number is missing on pages 1 and 2. The Specification has been amended at page 1, line 10 to address Examiner's objection. However, no reference to another application can be found on page 2 of the Specification.

Claim Rejections – 35 USC §112

Claims 5, 12, 22 and 24 are rejected under 35 U.S.C. § 112, second paragraph because of the term "about."

It is kindly asserted that usage of the term "about" in these claims does not render the claims indefinite.

The term "about five" envisions some amount of deviation from five. Words of approximation, such as "generally" and "substantially," are descriptive terms "commonly used in patent claims 'to avoid a strict numerical boundary to the specified parameter.'"; see, e.g., Andrew Corp v. Gabriel Elecs. Inc., 847 F.2d 819, 821-22 (Fed. Cir. 1988) (noting that terms such as "approach each other," "close to," "substantially equal," and "closely approximate" are ubiquitously used in patent claims and that such usages, when serving reasonably to describe the claimed subject matter to those of skill in the field of the invention and to distinguish the claimed subject matter from the prior art, have been accepted in patent examination and upheld by the courts). Anchor Wall Sys. v. Rockwood Retaining Walls, Inc., 340 F.3d 1298, 1310-1311 (Fed. Cir. 2003) (internal citations omitted).

Claim Rejections – 35 USC §101

Double Patenting

Claims 1-7 and 13-39 were provisionally rejected under the doctrine of double patenting over claims 7, 22, 23, and 31 of co pending Application No. 10/006,554. It is submitted that these claims are patentably distinct from the claims in the cited co-pending application, contrary to the Examiner's assertion. The Examiner recognizes that there are differences in the claims, but appears to assert that these differences are so insignificant as to not make any difference in terms of patentability. Firstly the differences sighted by the Examiner are significant. Secondly, there are additional differences in the claims that are apparently not recognized or appreciated by the Examiner. This can be seen in the Examiner's charts on pages 3 - 5 of the current Office Action. For example, among other numerous differences, claim 13 has "means for" terminology where as claim 23 does not. Therefore, by virtue of statute, for this reason alone claim 13 would likely be afforded a different scope than claim 23 under 35 USC § 112. As another example, claim 1 of the present application has a step of "authorizing the media" whereas claim 7 of the co pending application does not have any similar limitation. This is a significant and non-trivial step in safeguarding content, and is described in detail in the detailed description of the preferred embodiments. According to the Federal Circuit, double patenting is an affirmative defense, and must be proven by clear and convincing evidence, "a heavy and unshifting burden." See Symbol Technologies, Inc. v. Opticon, Inc. 935 F.2d 1569 (Fed. Cir. 1991). It is submitted that the cited claims have differences from each other that are not insubstantial or obvious, and that Examiner's charts, to the contrary of providing clear and convincing evidence of double patenting, illustrate the numerous differences between the compared claims. Therefore, it is kindly asserted that the claims are not, as submitted or as amended, invalid due to the judicially created doctrine of double patenting.

Claim Rejections – 35 USC §103

Claims 1, 5-7 and 13-32:

Claims 1, 5-7 and 13-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,832,293 to Tagawa et al. ("Tagawa") in view of U.S. Patent No. 5,604,801 to Dolan et al. ("Dolan").

Claim 1 recites:

1. A method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising:
 - authorizing the media;
 - decrypting the track by a process comprising:
 - (a) calculating a media unique key; and thereafter
 - (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter
 - (c) decrypting a group of frames; and thereafter
 - (d) deleting the decrypted title key;
 - (e) deleting the media unique key; and
 - (f) repeating (a) through (e) until the entire track is completed.

Tagawa, alone or in combination with Dolan, does not teach all of the elements of claim 1. The Examiner states that Tagawa teaches “(b) decrypting a title key stored in the memory of the device with the media unique key” at Col. 9, lines 14-29. To the contrary, Tagawa does not teach this claim limitation but teaches that a file key is *encrypted* based on the media ID at Col. 9, lines 14-29. Firstly encrypting is the opposite of decrypting. Secondly, the claimed media unique key is not simply a media ID. Thirdly, a piece of information used to create an encryption key is not necessarily required to decrypt the key. Therefore, the teachings of Tagawa, alone or in combination with Dolan, neither explicitly nor inherently teaches claim element (b).

The Examiner relies on Dolan for the teachings of limitations (d), (e), and (f) of claim 1. Dolan, however, does not teach those limitations.

In Dolan, the “invention is directed to the problem of providing a secure method of enabling messages to be processed using public key processing on behalf of the authorised holder of a portable security device, such as a smart card, in such a manner that it can be shown that only the authorised holder of the security device could have authorised the processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device.” Col. 2, lines 54-64.

Dolan in no way teaches a method of accessing an encrypted track on a removable media with a device, the track comprising frames having content. Dolan has nothing to do with tracks, whether audio or video, and accessing such tracks when they are in encrypted form on a removable media. Dolan teaches a data communications system in which messages are processed using public key cryptography with a private key unique to one or more users 150 under the control of a portable security device 120, such as a smart card, held by each user. Abstract. In Dolan, a workstation 110 incorporating a smart card reader for operation in conjunction with smart card 120 is connected to network 100 as is a server computer 130 and another computer 140 that is the intended recipient of the message. See Col. 5, lines 23-35. Dolan teaches that this system could be used to certify a message such as a debit instruction for the users account, and that generation of a digital signature is performed by server 130. See Col. 5 lines 30-38.

A public key data communications system is very different in purpose and form than the claimed method of accessing an encrypted [audio or video] track. Much of the security in such a public key system like that taught in Dolan comes from the server. The Examiner cites lines 11-14 of Column 3 of Dolan as teaching the claimed limitations of “(d) deleting the decrypted title key; (e) deleting the media unique key; and (f) repeating (a) through (e) until the entire track is completed.” Dolan does not teach a title key in the cited region or elsewhere. Nor does Dolan teach a decrypted title key, or in turn deleting a decrypted title key. Furthermore, the key the Examiner appears to equate with the claimed title key is on a server in Dolan, not on workstation 110 in Dolan which *might* be equated with the claimed device, or smart card 120 which *might* be equated with the removable media. The private key of the public/private key pair that the Examiner appears to equate with the claimed title key in the disputed limitation, is taught to be on a server in Dolan, not on the user device or removable media (smart card in Dolan).

Additionally, Dolan does not teach a media unique key of claim element (e), or deleting such a media unique key. Finally, as previously mentioned, Dolan does not teach a track. Dolan therefore cannot also teach claim element (f) of “repeating (a) through (e) until the entire track is completed.”

The Examiner’s interpretation of “after use” as “until the entire track is completed” on page 7 of the Office Action cannot stand. Firstly, it is an incomplete assertion and ignores the

repeating of steps (a) through (e), which is not a superfluous part of step (f) and the overall process and involves performing complex processes in an orderly fashion. Secondly, there is no basis within Dolan that can support such an interpretation. As mentioned above, Dolan does not teach a track of any kind, let alone repeating steps (a) through (e) until the entire track is completed. This interpretation appears to rely on the benefit of hindsight.

Furthermore, even if the combination of Tagawa and Dolan did teach all the limitations of claim 1, one of skill in the art would not be motivated to make such a combination.

First, as a threshold matter, Dolan is not analogous art and one of skill in the art would therefore not look to Dolan in solving the particular problem at hand. As seen above, Dolan deals with a completely different problem than the claimed invention(s) and described embodiments. The Public Key Data Communications System of Dolan is not relevant to the problem and solution claimed in the present invention, as discussed above (please refer to each claim individually, each of which covers different aspects of the solution and speaks for itself).

Second, there are no specific teachings in either Dolan or Tagawa that would lead one of skill in the art to combine the teachings of the references to arrive at the invention recited in claim 1. Claim 1 is very different than Dolan's public key structure that relies on servers with keys in controlled environments to certify messages such as the type used in transactions and other debits. The teachings of Dolan are also quite different than those of Tagawa, and there is nothing in the teachings of either reference that would lead one of skill to combine the teachings of one reference with the teachings of the other reference.

It seems therefore that such a combination can only be made with the benefit of hindsight, which is impermissible.

Furthermore, in addition to not being particularly relevant to the problem at hand, Dolan actually teaches away from the claimed invention and one of skill in the art would not be motivated to combine its teachings with those of Tagawa. As mentioned above, Dolan teaches "processing of a particular message, without requiring the public key algorithm to be performed by the security device, without having to store the private key in the security device, and without requiring the key generation process to be performed by the security device." Col. 2, lines 54-64.

Therefore, it is submitted that Tagawa, alone or in combination with Dolan does not and cannot render claim 1 obvious under § 103 of 35 USC.

Claims 5-7 depend from claim 1 and are allowable for all the reasons above regarding claim 1.

In addition, claim 5 recites that “the group of frames comprises less than one to about five seconds of content in a decoded or decompressed form.” Tagawa, alone or in combination with Dolan, does not teach this. The Examiner has cited Column 15 lines 59-65 of Tagawa for this proposition, but is kindly asserted that neither the cited portion nor any other portion of Tagawa teaches this claim limitation. While Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a maximum playback period of 8.4 minutes (Col. 15, lines 32-34), it does not teach, either explicitly or inherently, “the group of frames [decrypted at a time in element (c)] comprises less than one to about five seconds of content in a decoded or decompressed form.” Tagawa is silent on how much content is copied and decrypted at a time, and therefore how long any key may be in a vulnerable decrypted state.

Independent claim 13 is reproduced below.

13. A system for enabling a device to read an encrypted file having encrypted content from a media, and to write an encrypted file having encrypted content to a media, the system comprising:

a computing unit, and a system memory;

interface means for receiving commands from the device;

secure dynamic decryption means configured to:

(a) copy an encrypted title key from the media to a memory of the device,

(b) decrypt the encrypted title key,

(c) decrypt a portion of encrypted content with the decrypted title key,

(d) delete the decrypted title key, and

(e) repeat a-d such until all of the content of the file has been decrypted, and

wherein the decrypted title keys reside in and are accessible only to the secure means of the system.

Tagawa, alone or in combination with Dolan does not teach all of the limitations of independent claim 13. Tagawa, alone or in combination with Dolan does not teach the repetition of steps (a)-(d) and all of the processes that it entails. Again, while Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a

maximum playback period of 8.4 minutes (Col. 15, lines 32-34), it does not teach, either explicitly or inherently the repetition of steps (a)-(d) and all of the processes that it entails.

Furthermore, for all the reasons given above, the two references cannot be properly combined because Dolan is not analogous art, because there is not proper motivation to combine, and because Dolan teaches away from the claimed combination and from Tagawa.

Additionally, neither Tagawa nor Dolan teaches the claim 13 limitation “wherein the decrypted title keys reside in and are accessible only to the secure means of the system.” The secure means referred to is the secure dynamic decryption means that is configured to perform the enumerated steps (a)-(e). As discussed above, neither Tagawa nor Dolan teaches such a means. Nor do they teach the limitation “wherein the decrypted title keys reside in and are accessible only to the secure means of the system.” The title key is decrypted in step (b) once it has been copied from the media to a memory of the device in step (a). This decrypted key or keys are not taught to reside in this or other secure means of Tagawa or Dolan. The cited portion of Dolan (Col. 2 lines 27-28) that teaches that compromised keys can be used by a different user to process messages has little relevance to the decryption means that is configured to perform the enumerated steps (a)-(e), and does not render any of the limitations of claim 13 obvious.

Dependent claim 14 recites that “the title key is in a decrypted state for the time it takes to decrypt 5 seconds or less of content in a decompressed and decoded state when played back.” This is not taught by Tagawa and Dolan. As discussed above, while Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a maximum playback period of 8.4 minutes (Col. 15, lines 32-34), it does not teach this limitation. This is also true for dependent claim 22.

Dependent claim 15 recites: “the system of claim 13, further comprising a digital signal processor.” Note that this is in addition to the recitation of a computing unit in independent claim 13. The Examiner has cited Col. 8, lines 41-50 and Col. 55 lines 1-5 as teaching this limitation. Neither the cited portion, nor any other portion of Tagawa teaches this claim limitation. Col. 55 lines 1-5 teach that the audio can be in AAC, MP3 or other formats. Col. 8 lines 41-50 teaches about the sectors and storage capacity of a card. None of this explicitly or inherently teaches a digital signal processor.

Dependent claim 18 recites “the system of claim 15, wherein the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital

signal processor.” As discussed regarding claim 15, the digital signal processor is in addition to the claimed computing unit, and the cited references do not teach a digital signal processor. The cited references also do not teach that “the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor.” In fact, the Examiner relies on Col. 41, lines 32-33 to render obvious claims relating to the computing unit in claims 17 and 28, and also claims to render obvious claims relating to the digital signal processing unit in claims 18 and 19. Col. 41 lines 32-33 does not explicitly or inherently teach the distinct elements of a digital signal processor or a computing unit and the functions they are claimed to perform.

Independent claim 20 is reproduced below.

20. A system that enables a device to decrypt a file having encrypted content on a secure medium, the system comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium;

a security engine for decrypting the encrypted content and the one or more encrypted keys sent from the secure medium to a memory of the device, the decrypted keys used to decrypt the encrypted content, wherein

the one or more keys are contained in an encrypted data segment, and

the security engine (a) decrypts one or more of the keys, (b) decrypts a portion of the encrypted content using the one or more decrypted keys, and (c) deletes the one or more decrypted keys, and (d) repeats (a) - (c) until all portions of the content are decrypted.

Tagawa, alone or in combination with Dolan, does not teach the claim 20 limitation of “an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium.”

There is no indication of usage of an application programming interface in Tagawa. As seen in *The Free On-line Dictionary of Computing*, © 1993-2005 Denis Howe, available at www.dictionary.com, an application programming interface, or “API” is understood by those of skill in the art to mean:

<programming> (API, or "application programming interface")

The interface (calling conventions) by which an application program accesses operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure the portability of the code.

An API can also provide an interface between a high level language and lower level utilities and services which were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main task may be the translation of parameter lists from one format to another and the interpretation of call-by-value and call-by-reference arguments in one or both directions.

Again, neither Tagawa nor Dolan teach the aforementioned limitations that include an API.

Also, Tagawa, alone or in combination with Dolan, for reasons previously discussed, fails to teach the limitation that "the security engine (a) decrypts one or more of the keys, (b) decrypts a portion of the encrypted content using the one or more decrypted keys, and (c) deletes the one or more decrypted keys, and (d) repeats (a) - (c) until all portions of the content are decrypted."

Dependent claim 23 recites that "the data segment comprising the one or more encrypted keys is buffered and decrypted in fractional portions." This is not taught by Tagawa and Dolan. None of the cited portions of Tagawa, nor any other portion of Tagawa teaches this explicitly or inherently. In particular, Col. 12 lines 1-12, cited by the Examiner, appears to be teaching about content, not keys. The cited portions of Columns 9 and 41 discuss file keys, but never teach that "the data segment comprising the one or more encrypted keys is buffered and decrypted in fractional portions."

Dependent claim 24 adds to dependent claim 23 that "the fractional portion is about 512 bytes." This is also not taught by Tagawa and Dolan. The Examiner relies on Col. 17 lines 60-64 for this teaching. However, Tagawa appears to be teaching that track text information may have a size of 512 bytes, not the claimed "data segment comprising the one or more encrypted keys [] buffered and decrypted in fractional portions."

Dependent claim 26 adds to claim 20 that “the device further comprises a digital signal processor.” Dependent claim 29 adds to claim 26 that “the system is stored in RAM of the digital signal processor.” Tagawa does not teach usage of a DSP, or either of these two claim limitations. Note that these claims are distinct from claim 28 “wherein the software system stored in the system memory is executed by the computing unit.”

Dependent claim 30 depends from claim 26 and recites that “a portion of the system is stored in the system memory of the device and a portion of the system is stored in RAM of the digital signal processor.” Again, this is not taught by Tagawa, alone or in combination with Dolan.

Dependent claim 32 adds that “the portion of the system stored in the RAM of the digital signal processor comprises the security engine.” This is also not taught by Tagawa and Dolan.

Therefore, for all the reasons above, it is kindly submitted that claims 1, 5-7 and 13-32 are not obvious and are in condition for allowance.

Claims 2-4, 8-12 and 38-39:

Claims 2-4, 8-12 and 38-39 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tagawa in view of Dolan and in further view of U.S. Patent No. 6,367,019 to Ansell et al. (“Ansell”).

Claim 2 is dependent on claim 1 and recites that authorizing the media comprises:
calculating a media key; and thereafter
calculating a media unique key from the media key; and thereafter
deleting the media key; and thereafter
calculating a session key from the media unique key; and thereafter
deleting the media unique key.

Claim 2 is in condition for allowance for all the reasons regarding claim 1. Additionally, the combination of Tagawa, Dolan, and Ansell does not teach all of the additional elements of dependent claim 2. It is unclear in the rejection of any of the claims that recite a media key and/or a media unique key what the examiner equates to be each of these distinct entities within each of the different cited references. This is further confused because the Examiner at different points indicates that manipulation of the same claimed element occurs within two different

references, even though the Examiner never specifies what equates to the claimed element in the different references. In particular, the Examiner has indicated that calculating a media key is taught by Tagawa, but that deleting the [calculated] media key is taught by Dolan. In the rejection of claim 2 the Examiner apparently takes an even greater leap by extending this complex series of calculations into a third reference, Ansell. The Examiner indicates that Ansell teaches calculating the claimed session key, which per the claim is specified as calculated from the media unique key, which in turn was calculated from the media key. Ansell teaches no such thing. Ansell teaches that “player 110 encrypts the media master key using a session key formed at the onset of a secure communication session between player 110 and portable player 150.” This does not teach “calculating a session key from the media unique key.” It appears to teach the opposite, but again this is unclear because the Examiner has not indicated any teachings that would lead one to equate the media master key of Ansell with a media unique key that was calculated by another distinct claim element, the media key. The Examiner indicates on page 15 of the Office Action that “calculating is interpreted as decrypting” and cites Col. 7, line 19 for this proposition. However, Col. 7, line 19 of Ansell teaches encrypting.

Therefore, the combination of Tagawa, Dolan, and Ansell does not teach all of the elements of claim 2, and cannot render the instant claim obvious. Furthermore, one of skill in the art would not be motivated to combine the teachings of all three references. As discussed previously, Dolan is not analogous art or pertinent to the problem at hand, and in fact teaches away from Tagawa. It is kindly submitted that the combination of all three of these references would not occur without the benefit of hindsight.

Claim 3 depends from claim 1 and recites “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key; and copying the singly encrypted title key from the media into a memory of the device.” The Examiner again relies on the combination of Tagawa, Dolan, and Ansell to render claim 3 obvious. Examiner also relies upon the same portion of Ansell, which teaches encrypting. Ansell simply does not teach “decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key.” Nor does it teach “copying the singly encrypted title key from the media into a memory of the device.” The Examiner states that “this modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so... in order

[not] to have a secure communication between the media and the device.” It is submitted that this is based on hindsight. Secure communication can be accomplished in any number of ways, and nothing in Ansell teaches or suggests the claimed solution.

Claim 4 depends from claim 2, and recites that calculating the media key comprises:

- (a) reading a first record of a media key block from a buffer;
- (b) updating the buffer offset based on the length and type of the first record;
- (c) reading another record of the media key block at the updated buffer offset; and
- (d) repeating (a) - (c) until all necessary records of the media key block are read and the media key is calculated.

The combination of Tagawa, Dolan, and Ansell does not teach all of the limitations of claim 4. None of these references teach a media key block. Page 11 of the application teaches about a media key block, and the paragraph beginning on about line 3 is reproduced below for the Examiner’s convenience.

The media key block (MKB), as stored in the system area 43 of the card memory, contains a sequence of contiguous records, one such record being illustrated in Figure 4. The entire MKB image 49 is 64 Kbytes. It is broken into 128 chunks of 512 bytes, and chunk 1, which contains all or part of they first record, and is labeled MKB chunk 50 in the figure, is enlarged to show its component parts. Chunk 50 may also contain multiple records. A first field 51 contains the record type, a second field 53 the total length of the record, and the remaining field 55 the key itself. The data in the record type and length fields 51 and 53 are not encrypted. Each record of the MKB is a multiple of 4 bytes in total length. As illustrated by a block 57 of Figure 5, the MKB key records are decrypted by device keys stored in the portable device (PD), licensed compliant module (LCM) or other device that utilizes a memory card for reading or programming content data stored on it. Device keys Kd1, Kd2, Kd3 ... are written into a memory of the utilization device, such as non-volatile flash memory within the MCU 25 of the portable audio player of Figure 2, by the manufacturer of the device. The device keys are provided to device manufacturers by the 4C Entity, and are maintained in confidence. The number of device keys which are stored in a given utilization device depends upon the type of the device.

Figure 10 describes the operation of processing the Media Key Block, and description of this processing can be seen at about pages 25-28 of the application.

Again, a media key block and the specific recitations of claim elements (a)-(d) are simply not taught by Tagawa, alone or in combination with the other references. For example, the

portion of Tagawa the Examiner cites (Col. 41, lines 25-29) for teaching element (d) teaches using a different file key for each AOB file. This is not relevant to claim 4.

Independent claim 8 is reproduced below.

8. (Original) A method of accessing an encrypted data file on a removable media with a device, the data file comprising frames having content, the method comprising:
authorizing the media for a user session by a process comprising:

calculating a media key; and thereafter

calculating a media unique key from the media key; and thereafter

deleting the media key; and thereafter

calculating a session key from the media unique key; and thereafter

deleting the media unique key.

decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key;

copying the singly encrypted title key from the media into a memory of the device; and
decrypting the file by a process comprising:

(a) calculating the media unique key; and thereafter

(b) decrypting the title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key;

(f) repeating (a) through (e) until the entire file is completed.

Claim 8 has limitations similar to claim 2 and claim 1 from which it depends, and is not obvious in light of the combination of Tagawa, Dolan, and Ansell for the reasons given above regarding claims 1 and 2.

Claim 9, as amended, depends from claim 8 and recites “calculating the media key comprises: dividing a media key block into chunks, the chunks comprising bytes of encrypted data; and decrypting a key within the media key block by setting the buffer to read at an offset within a specific chunk of the block.” Claim 9 is not obvious for all the reasons regarding claim 8. Furthermore, Tagawa does not teach all of the limitations of dependent claim 9. In addition

to not teaching a media key block itself, Tagawa does not teach the claimed manipulation of a media key block. The Examiner appears to equate the encryption key storing file “AOBSA1.KEY” taught at lines 59-64 of Tagawa with the claimed media key block. It is not the same as the claimed media key block. The Examiner is kindly requested to refer to the discussion above regarding claim 4 for information regarding the media key block, and calculation/manipulation of the media key block. Furthermore, even if Tagawa does teach the claimed media key block, it does not teach “dividing a media key block into chunks, the chunks comprising bytes of encrypted data; and decrypting a key within the media key block by setting the buffer to read at an offset within a specific chunk of the block.”

Claim 10, as amended, depends from claim 9 and recites that “decrypting the key comprises:

- (a) calculating a media key from a first record; and
- (b) updating the buffer offset; and
- (c) reading a second record at the updated buffer offset; and
- (d) verifying the media key with a second record by comparing the calculated media key with a reference media key.”

Claim 10 is allowable for all of the reasons regarding the base claims from which it depends. Furthermore, Tagawa, Dolan, and Ansell, alone or in combination, do not teach all the elements (a) – (d) of claim 10. This is best illustrated by looking at element (d), which refers to portions of the other elements. As best as can be deciphered from the rejection of this claim, the Examiner takes the mention of a two-step encryption process where data is encrypted with a file key that is itself encrypted based on the media ID to teach element (d). This does not teach element (d) or any of the other claimed elements. The Examiner is kindly requested to explain what exactly he equates in the cited references with the claim elements so the rejection can be better understood.

Additionally, even if the combination of Tagawa, Dolan, and Ansell did teach all of the limitations of claim 10, one of skill in the art would not be motivated to combine all three of these references. As mentioned previously, Dolan is not analogous art, not pertinent to the problem at hand, and in fact teaches away from the claimed combination and the other references.

Claim 11 depends from claim 10 and recites “the buffer offset is determined by the type and length of the first record of the media key block.” The combination of Tagawa, Dolan, and Ansell does not teach a media key block and different types and lengths of records of a media key block. Additionally, even if the combination of Tagawa, Dolan, and Ansell did teach all of the limitations of claim 11, one of skill in the art would not be motivated to combine all three of these references. As mentioned previously, Dolan is not analogous art, not pertinent to the problem at hand, and in fact teaches away from the claimed combination and the other references.

Claim 12 depends from claim 8 and recites “group of frames comprises less than one second to about five seconds of decompressed and decoded audio content. As discussed above, while Tagawa does teach that an AOB element has a playback period of around two seconds and that an AOB block has a maximum playback period of 8.4 minutes (Col. 15, lines 32-34), it does not teach this limitation.

Claim 38 depends from claim 20 and recites “the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number.” The combination of Tagawa, Dolan, and Ansell does not teach this. The portion of Ansell cited by the Examiner teaches a first and presumably second random number. It does not teach generating those number(s) with “a random number generator, the generator utilizing two or more system timers to create the random number.” Additionally, even if the combination of Tagawa, Dolan, and Ansell did teach all of the limitations of claim 38, one of skill in the art would not be motivated to combine all three of these references. As mentioned previously, Dolan is not analogous art, not pertinent to the problem at hand, and in fact teaches away from the claimed combination and the other references.

Claim 39 depends from claim 38 and recites “the generator increases the natural frequency update of the timer ticks used to create the random number.” This is also not taught by the combination of Tagawa, Dolan, and Ansell. Additionally, as mentioned previously, even if the combination of Tagawa, Dolan, and Ansell did teach all of the limitations of claim 38, one of skill in the art would not be motivated to combine all three of these references.

Therefore, for all the reasons above, it is kindly submitted that claims 2-4, 8-12 and 38-39 are not obvious and are in condition for allowance.

Claims 33-34 and 36-37

Claims 33-34 and 36-37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tagawa in view of Dolan in further view of U.S. Patent Publication No. 2003/0014371 to Turgeon ("Turgeon").

Claim 33 is dependent upon claim 20 and recites "one or more engines for processing and transmitting audio, video or images, each engine comprising a secure application programming interface, the secure interface(s) for accessing the encrypted content and keys of the medium, and the non-secure interface(s) for accessing the unencrypted content of the medium." The combination of Tagawa, Dolan, and Turgeon, does not teach all of the elements of the claim. In particular, the combination does not teach at least "a secure application programming interface...". As seen in *The Free On-line Dictionary of Computing*, © 1993-2005 Denis Howe, available at www.dictionary.com, an application programming interface, or "API" is understood by those of skill in the art to mean:

<programming> (API, or "application programming interface")

The interface (calling conventions) by which an application program accesses operating system and other services. An API is defined at source code level and provides a level of abstraction between the application and the kernel (or other privileged utilities) to ensure the portability of the code.

An API can also provide an interface between a high level language and lower level utilities and services which were written without consideration for the calling conventions supported by compiled languages. In this case, the API's main task may be the translation of parameter lists from one format to another and the interpretation of call-by-value and call-by-reference arguments in one or both directions.

Even if the combination of Tagawa, Dolan, and Turgeon did teach all of the elements, one of skill in the art would not be motivated to combine these references. Turgeon is not analogous art and not relevant to the problem at hand. According to Turgeon:

[0002] The present invention relates generally to electronic commerce and financial transactions. More particularly, the present invention relates to a system and method for providing secure environment to carry out electronic payments or other financial transactions over the Internet or other open network using the

existing secure network, such as the automated teller machine (ATM) or point-of-sale (POS) network maintained by NYCE.RTM., CIRRUS.RTM., etc.
It is an object of the present invention to provide a secure environment for financial services conducted over a public network.

[0010] It is another object of the present invention to provide a method for purchasing goods or services on-line.

[0011] It is yet another object of the present invention to authenticate on-line users conducting financial services over a public network.

[0012] The above and other objects are achieved by a system for providing financial transactions over a public network accessible by customers via respective network access devices with modems and over a private network accessible by financial institutions via computers with modems.

This has very little if anything to do with the problem addressed in and the teachings of Tagawa and the present invention. Therefore, one of skill in the art would not combine the teachings of Turgeon with those of Tagawa. As mentioned previously, one of skill in the art would also not be motivated to combine the teachings of Dolan with those of Tagawa.

Claim 34 depends from claim 33 and is allowable for all the reasons of the claims from which it depends.

Claim 36 depends from claim 33 and recites "the system of claim 33, further comprising a device driver, the security engine accessing the content and keys through the device driver." Tagawa, alone or in combination with Dolan and Turgeon does not teach this limitation. The Examiner appears to be citing the teachings of insertion slot and/or memory card 31 of Tagawa Fig 48 for these teachings. However, this or anything else in cited references do not teach "a device driver, the security engine accessing the content and keys through the device driver." Also, as mentioned above, one of skill in the art would not combine the three references together.

Claim 37, as amended, depends from claim 33 and recites "wherein each of the one or more engines for processing and transmitting audio, video or images further comprises a non-secure application programming interface for accessing unencrypted content of the medium." As mentioned above, none of the cited references teaches an API, either explicitly or inherently.

Therefore, for all the reasons above, it is kindly submitted that claims 33-34 and 36-37 are not obvious and are in condition for allowance.

Claim 35

Claim 35 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tagawa in view of Dolan in view of Turgeon and in further view of Ansell

Claim 35 depends from claim 34 and recites "wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine." This claim is allowable for all the reasons regarding claim 34. The cited references do not teach an API and there is not proper motivation for combining the references. The references also do not teach that "the secure [application programming] interface(s) communicate with the security manager module and the module communicates with the security engine."

Information Disclosure Statement:


On October 22, 2004, Applicants filed an Information Disclosure Statement citing 27 references on 3 pages of the Form PTO 1449. The Examiner initialed all but reference numbers 1 and 2. Enclosed is a copy of the partially initialed Form PTO 1449 for the Examiner to initial and return with the next Action.

A Supplemental Information Disclosure Statement is also being filed herewith citing new references.

Conclusion

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

Respectfully submitted,

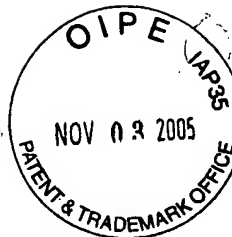


Gerald P. Parsons
Reg. No. 24,486
PARSONS HSUE & DE RUNTZ LLP
655 Montgomery Street, Suite 1800
San Francisco, CA 94111
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)

October 31, 2005

Date

**BOX MISSING PARTS
COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231**



COPY

Applicants: BAHMAN QAWAMI, FARSHID SABET-SHARGHI, ROBERT C. CHANG
 Assignee: SANDISK CORPORATION
 Title: SYSTEM, METHOD, AND DEVICE FOR PLAYING BACK RECORDED AUDIO VIDEO OR OTHER CONTENT FROM NON-VOLATILE MEMORY CARDS, COMPACT DISKS OR OTHER MEDIA
 Serial No.: 10/006,465
 Filed: December 6, 2001
 Atty Docket No.: M-9913-1 US

ENCLOSED:

1. This Return Receipt Postcard;
2. Response to Notice to File Missing Parts of Non-Provisional Application - Filing Date Granted (In duplicate)
3. Part 2 of Notice to File Missing Parts of Nonprovisional Application
4. Executed Declaration for Patent Application and Power of Attorney

PGM/tlk

May 6, 2002

EXPRESS MAIL LABEL NO.: EV029353786US

RECEIVED
BY DOCKET DEPT.
S.F.

MAY 15 2002



Q

SI



**POST OFFICE
TO ADDRESSEE**



EV 029353786 US

ORIGIN (POSTAL USE ONLY)	
Postage: 6/4/26	Day of Delivery: <input checked="" type="checkbox"/> Next <input type="checkbox"/> 2nd <input type="checkbox"/> 3rd
Date: 5/6/02	Flat Rate Envelope: <input type="checkbox"/>
Time: 1:37 PM	Postage: \$ 12.45
Weight: 3.0 lbs	Return Receipt Fee: <input type="checkbox"/>
Insurance: 0.00	Insurance Fee: <input type="checkbox"/>
Acceptance Clerk Initials: [Signature]	Total Postage & Fees: \$ 12.45

SEE REVERSE SIDE FOR
SERVICE GUARANTEE AND LIMITS
ON INSURANCE COVERAGE

WAIVER OF SIGNATURE (Domestic Only): Additional merchandise insurance is void if waiver of signature is requested. I wish delivery to be made without obtaining signature of addressee or addressee's agent (if delivery employee judges that article can be left in secure location) and I authorize that delivery employee's signature constitutes valid proof of delivery.

NO DELIVERY: ☐ Weekend ☐ Holiday ☐ Customer Signature: [Signature]

CUSTOMER USE ONLY

METHOD OF PAYMENT: **X951249**

Express Mail Corporate Acct. No.: **415 217 6000**

FROM: (PLEASE PRINT) **SKJERVEN MORRILL & MACPHERSON**
3 EMBARCADERO CTR STE 2800
SAN FRANCISCO CA 94111-4066

PHONE: **M-9913-1 US / P6M**
11587.00924

Federal Agency Acct. No. or Postal Service Acct. No.: **DC 20231-0001**

TO: (PLEASE PRINT) **COMMISSIONER FOR PATENTS**
WASHINGTON

BOX MISSING PARTS

Customer Copy
Label 11-F August 2000

F02
T12

321

FOR PICKUP OR TRACKING CALL 1-800-222-1811 www.usps.com



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): BAHMAN QAWAMI, FARSHID SABET-SHARGHI, ROBERT C. CHANG

Assignee: SANDISK CORPORATION

COPY

Title: SYSTEM, METHOD, AND DEVICE FOR PLAYING BACK
RECORDED AUDIO, VIDEO OR OTHER CONTENT FROM NON-
VOLATILE MEMORY CARDS, COMPACT DISKS OR OTHER
MEDIA

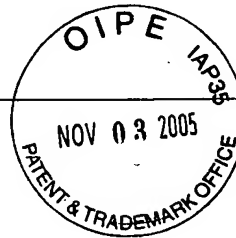
Serial No.: 10/006465

Filing Date: December 6, 2001

Examiner: Unknown

Group Art Unit: 2184

Docket No.: M-9913-1 US



San Francisco, California
May 6, 2002

BOX MISSING PARTS
COMMISSIONER FOR PATENTS
Washington, D.C. 20231

RESPONSE TO NOTICE TO FILE MISSING PARTS OF NON-
PROVISIONAL APPLICATION - FILING DATE GRANTED

Dear Sir:

In response to the "Notice to File Missing Parts of Non-Provisional Application - Filing Date Granted" mailed by the United States Patent and Trademark Office on March 5, 2002, the following documents are enclosed to complete the filing of the above-identified patent application:

1. A Declaration for Patent Application and Power of Attorney signed by the inventors in compliance with 37 CFR 1.63.
2. Copy of Notice to File Missing Parts of Non-Provisional Application - Filing Date Granted.

The United States Patent and Trademark Office is hereby authorized to charge the following fees to Deposit Account No. 19-2386:

LAW OFFICES OF
SKJERVEN MORRILL LLP
25 METRO DRIVE
SUITE 700
SAN JOSE, CA 95110
(408) 453-9200
FAX (408) 453-7979

- | | | |
|----|--|-----------|
| 1. | Surcharge for filing declaration on a date later than the filing date of the application | \$130.00 |
| 2. | TOTAL FEES: | \$ 130.00 |

The Commissioner is hereby authorized to charge any additional fees, which may be required, or credit any overpayment to Deposit Account No. 19-2386.

It is hereby respectfully submitted that the enclosed documents complete the filing of the above patent application and justify the filing date of December 6, 2001. Please telephone the undersigned at (415) 217-6000, if there are any questions. This form is being submitted in duplicate.

EXPRESS MAIL LABEL NO:

EV029353786US

Respectfully submitted,



Peter G. Mikhail
Attorney for Applicant(s)
Reg. No. 46,930

LAW OFFICES OF
SKJERVEN MORRILL LLP

25 METRO DRIVE
SUITE 700
SAN JOSE, CA 95110
(408) 453-9200
FAX (408) 453-7979

U.S. Department of Commerce, Patent and Trademark				Atty. Docket No.		Application No.		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary) (Form PTO-1449)				SNDK.315US2		10/006,465		
				Applicants		Conf. No.		
				Bahman Qawami et al.		3583		
				Filing Date		Art Group		
				December 6, 2001		2134		
U.S. Patent Documents								
*Examiner Initial		Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate	
	1	4,465,901	8/14/1984	Best				
U.S. Published Patent Application Documents								
*Examiner Initial		Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate	
	2	2001/0021255A1	9/13/2001	Ishibashi				
Foreign Patent Documents								
							Translation	
		Document	Date	Country	Class	Subclass	Yes	No
56	3	01/67668A	13/9/2001	WIPO			X	
	4	2,592,502	7/3/1987	France			Abstract	X
	5	3,601,526 A1	23/7/1987	Germany			Abstract	X
	6	3,512,785 A1	23/10/1986	Germany			Abstract	X
	7	0 198 384	22/10/1986	Europe			Abstract	X
	8	0 191 324 A2	20/8/1986	Europe			X	
	9	0 138 219 A2	24/4/1985	Europe			X	
56	10	87/05726	24/9/1987	WIPO			Abstract	X
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)								
56	11	IPEA/European Patent Office, "International Preliminary Examination Report", mailed in corresponding PCT/US01/47014, September 6, 2004, 5 pages.						
	12	ISA/European Patent Office, "International Search Report", mailed in corresponding PCT/US01/47014, August 18, 2004, 5 pages.						
	13	ISA/European Patent Office, "Partial International Search", mailed in corresponding PCT/US01/4661, August 18, 2004, 5 pages.						
	14	MMCA Technical Committee, "The MultimediaCard System Summary, Based on System Specification Version 2.2", www.verbatim.com.au/tecnotes/MMC_Rev 1.0.pdf, January 2000, pp. 1-27.						
56	15	Intel Corporation et al., "Content Protection for Recordable Media Specification: DVD Book", http://www.4centity.com/4centity/tech/cprm/, Revision 0.94, October 18, 2000, 46 pages.						
Examiner <u>Shawna G. Gelay</u> Date Considered <u>4/15/05</u>								
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.								